UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

CISCO SYSTEMS, INC and CISCO TECHNOLOGY, INC.,	:	
	:	19 Civ. _____
Plaintiffs,	:	
	:	**DECLARATION OF CHARLES WILLIAMS**
-against-	:	
	:	
SHENZHEN TIANHENG NETWORKS CO; GEZHI PHOTONICS TECHNOLOGY CO., LTD ; SHENZHEN SOURCELIGHT TECHNOLOGY CO.; HU JIANGBING; LI PAN; DONG DAOSHUN; WANG WEI; and DARIOCOM,	:	**FILED *EX PARTE* AND UNDER SEAL PURSUANT TO 15 U.S.C. § 1116**
Defendants.	:	

Charles Williams, pursuant to 28 U.S.C. § 1746, hereby declares as follows:

1. I am familiar with the matters set forth in this declaration based upon my own personal knowledge. If called as a witness, I could and would competently testify to the following facts.

2. I submit this declaration in support of Plaintiffs' Order to Show Cause.

3. I am employed by Cisco Systems, Inc ("Cisco") as a Director with the Brand Protection Organization. I have been employed by Cisco since 1999, and with Brand Protection since 2004. My job responsibilities include managing Cisco's brand protection team in the Americas, including managing counterfeit investigations. This declaration is based on my personal knowledge and/or information contained in the normal business of Cisco and Cisco Technology, Inc., to which I have access as part of my duties. I am fully familiar with the facts discussed below.

Cisco's Registered Trademarks Are Invaluable

4. Cisco was founded in 1984 and is the worldwide leader in developing, implementing, and providing the technologies behind networking, communications, and information technology products and services. Cisco develops and provides a broad range of networking products and services that enable seamless communication among individuals, businesses, public institutions, government agencies, and service providers. Specifically, the thousands of engineers who work at Cisco develop and provide networking and communications hardware, software, and services that utilize cutting-edge technologies to transport data, voice, and video within buildings, across cities and campuses, and around the world.

5. Since its founding, Cisco has invested heavily in the CISCO brand, which includes the CISCO word mark and the following CISCO logos (together, the "CISCO Marks"):

6. Cisco has used—and is currently using—the CISCO Marks continuously and exclusively in commerce and in connection with networking hardware, including pluggable transceiver modules ("Cisco transceivers").

7. Attached as **Exhibit 1** are true and correct copies of registration certificates for the CISCO Marks.

8. Cisco prominently displays the CISCO Marks in its advertising and promotional materials. As a result of extensive promotion and widespread sales, the CISCO Marks are widely recognized and have become well known to the public and synonymous with reliable, high-quality networking hardware products. Cisco has spent, and continues to spend, billions of dollars

marketing and promoting in interstate commerce these products in connection with the CISCO Marks.

9. Due to Cisco's longtime use of and investment into the CISCO Marks and the quality of Cisco's products, the Cisco brand has built up a tremendous amount of consumer goodwill. The CISCO Marks symbolize business goodwill of Cisco and are invaluable assets to Cisco

10. In 2018, Interbrand ranked Cisco as the fifteenth most valuable brand in the world, with an estimated value of over $34.5 billion. The volume of Cisco's annual sales revenue of hardware, software, and related services is approximately $50 billion worldwide. Cisco ships over 10 million transceivers per year

Critical Infrastructures Are Built on Cisco Transceivers

11. As a leading provider of networking gear, Cisco and its transceivers are critically responsible for the networks in the United States and around the world. Performance of a network is dependent on the transceiver. Cisco transceivers provide the central link or connection.

12. Cisco's transceivers are purchased and used by the U.S. government, hospitals, utilities, transportation services, the education industry, communication service providers, financial services, professional services, and other industries. These industries use Cisco's products in critical and life-essential applications. Governmental and other infrastructures are built on, and rely upon, Cisco products to maintain the security of data storage and ensure the integrity of data transfer and communications. Many critical government functions rely upon the performance of high-quality Cisco products, as compared to the dangers posed by low-quality counterfeits.

13. In fact, the U.S. military and its members critically depend on authentic Cisco products. In a federal criminal action brought by the U.S. government against a counterfeiter of Cisco networking hardware, *United States v Ehab Ashoor*, No. H-09-CR-307 (S.D. Tex.), U.S. Marines Staff Sergeant Lee Chieffalo testified before a jury concerning the U.S. military's extensive use of and reliance on Cisco products to transfer and receive data. As explained by Staff Sergeant Chieffalo, "[t]he Marine Corps' network infrastructure is solely Cisco equipment," and "the equipment that Cisco uses has proprietary protocols and software on them that operates only with other Cisco gear." That Cisco gear is "built to specifications that [the Marine Corps] use[s] for reliability and environmental hardness." The Marine Corps utilizes the Cisco-based classified network for all of its battle operations, including sharing intelligence, convoy operations, troop movements, air operations, call for fire, and medevacs. The risk, according to Staff Sergeant Chieffalo, of using substandard counterfeit products could not be higher: "Marines could die." A true and correct copy of excerpts of Staff Sergeant Chieffalo's sworn testimony are attached as **Exhibit 2**.

14. Understanding the grave risks posed by counterfeit Cisco products, the U.S. government, from 2005 to 2010, conducted a coordinated law enforcement operation concerning counterfeit Cisco networking products, called "Operation Network Raider." This effort was led by the Department of Justice, with investigative support by the FBI, Homeland Security, and various Office of Inspector General offices representing the Department of State, Department of Defense, and other government entities. As stated in a press release issued by the Department of Justice on May 6, 2010, "Operation Network Raider, a domestic and international enforcement initiative targeting the illegal distribution of counterfeit network hardware manufactured in China, has resulted in 30 felony convictions and more than 700 seizures of counterfeit Cisco network

hardware and labels with an estimated retail value of more than $143 million." Emphasizing the public security aspect of counterfeit networking products, John Morton, Assistant Secretary of Homeland Security, explained: "These cases involve greedy businessmen hocking counterfeit and substandard hardware to any buyer—whether it could affect the health and safety of others in a hospital setting or the security of our troops on the battlefield.... They pose a triple threat to our nation by stealing from our economy, threatening U.S. jobs and potentially putting the safety of our citizens at risk." A true and correct copy of this press release is attached as **Exhibit 3**. Since 2010, there have been other criminal cases involving counterfeit Cisco products.

Defendants' Counterfeiting Harms Consumers and Cisco

15. Defendants trade off the goodwill associated with the CISCO Marks and deceive consumers into believing the counterfeit Cisco products were manufactured or authorized by Cisco, resulting in harm to Cisco and consumers

16. None of the defendants in this matter have ever been authorized to reproduce or use the CISCO Marks in connection with the sale of counterfeit products. The "Cisco" products the defendants distribute, offer for sale, and sell are counterfeit products that are confusingly similar to Cisco's own authentic product; bear counterfeit and confusingly similar imitations of the CISCO Marks, and are not manufactured by Cisco or any party associated or affiliated with, or authorized, licensed, or approved of by Cisco.

17. Cisco requires its original equipment manufacturers ("OEMs") to follow strict quality and control standards, which govern everything from the design of the product and the selection of components, to production in a clean facility and ongoing reliability testing, audits, and recordkeeping. Unfortunately, if these standards are not followed and any necessary steps in

sourcing, manufacturing, and distributing the transceivers are compromised or not followed, the product may not function properly and may be unsafe to operate.

18. The manufacturers of the counterfeit transceivers are not subjected to any of these standards, and in light of the substantially lower prices the counterfeiters charge and the differences between the authentic and counterfeit products, it is a certainty that they do not follow any such standards concerning design, testing, manufacturing, and distribution. Investigations by Chinese law enforcement into other counterfeiting manufacturing operations have confirmed this, revealing operations that are extremely rudimentary and do not meet any of Cisco's manufacturing, safety, or cleanliness standards.

19. Defendants' conduct harms Cisco because counterfeit Cisco products that fail or degrade create the false impression that Cisco products are unreliable. This improperly tarnishes Cisco's reputation and causes Cisco to suffer lost sales and future business opportunities. As a result, Cisco suffers substantial and irreparable harm to its brand, image, business, and goodwill with the public.

20. The sale of counterfeit Cisco also harms the OEMs that manufacture the transceivers. The financial health of these OEMS is essential to ensure a steady stream of high-quality components and products that can be relied upon by Cisco and its customers. The presence of counterfeits likewise causes OEMs to lose sales and business opportunities, which can put their financial health at risk.

21. Most importantly, defendants' conduct harms consumers who are deceived and receive low-quality counterfeit products instead of high-quality genuine Cisco products. The risks presented by counterfeit products are very real. If non-approved components are used in the product, there is a risk the product will not function properly and will not function in combination

with authentic Cisco products and components being used in the network. Moreover, while Cisco products are manufactured and updated with the latest software, counterfeit products that use pirated versions of earlier and outdated software may not operate correctly, and may leave users exposed to security and intrusion vulnerabilities that were detected and fixed in more current versions of the software. Because this substandard operation may not be apparent to the consumer, the consumer may believe its network is protected, when in reality improper software is leaving dangerous gaps in the security.

22 These risks and the attendant harm are particularly pronounced with counterfeit transceivers. Transceiver quality and reliability is extremely important, and is the reason Cisco invests heavily in the quality and reliability of its products. Data integrity is critical to not only businesses, but to government, military, financial services, healthcare, energy and utilities, and transportation networks, all of which need to reliably transmit and receive data. Counterfeit transceivers put these consumers' data integrity in jeopardy. Furthermore, Cisco transceivers use different transmitter laser technologies, which require extensive eye safety testing and manufacturing calibration in order to ensure eye safety. Counterfeit transceivers may not be subjected to this testing or meet federal eye safety specifications. Finally, electromagnetic interference is another critical issue. A poorly designed transceiver can emit excessive electromagnetic energy that can interfere with adjacent equipment. This can be detrimental in any environment where sensitive electronic equipment is present, including in a military command, hospital, or data center.

23. Based on my 15 years of experience dealing with Cisco counterfeiters, it is crucial that the sale of counterfeit Cisco transceivers be stopped immediately.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on November 19, 2019

Charles Williams